UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/841,965	04/25/2001	Markus Baumeister	DE000071	6068

24737 7590 11/28/2005

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 11/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/841,965
Filing Date: April 25, 2001
Appellant(s): BAUMEISTER ET AL.

MAILED
NOV 2 8 2005
Technology Center 2100

Kenneth D. Springer
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed August 17, 2005 appealing from the office action mailed June 08, 2005.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, and judicial proceedings which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been entered.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

No evidence is relied upon by the examiner in the rejection of the claims under appeal.

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

2. **Claims 1, 3 and 4 and 7 are** rejected under 35 U.S.C. 102(a) as being anticipated by Peterka, (hereinafter referred as Peterka)(International Publication Number: WO 99/66714)

3. **As per claim 1 and 7 Peterka discloses**

- A network comprising terminals and a software system distributed over all the terminals, (page 13, lines 6-8; page 14, lines 20-24; figure 1, ref. Num "100", ref. Num "120"; ref. Num "160")(A network or the digital television broadcast network has the software system or the software application distributed or broadcasted to each terminals or receivers as explained on page 14, lines 20-24; the terminal is interpreted as "television receiver" and this interpretation is given in light of the submitted application as it is defined on page 3, lines 1-3) and

- At least an access controlled object (page 15,
lines 2-6; page figure 2, ref. Num "161" ; page 17, lines 27-31; page 18, lines 1-3; page

18, lines 24-29) (the "controlled objects" is interpreted by the office to be the "receiver functionalities or resources and/or user data" that are invoked or accessed in the terminal or in side the receiver at the block called "receiver function" as shown on figure 2, ref. Num "161" by either the software application file or "software system" as explained on page 15, lines 2-6; page 17, lines 18-31. In response to the software distributed over the terminals or the receiver, application execution module which is shown on figure 2, ref. Num "230" tries to invoke or access a receiver function including access to user private data as explained on page 17, lines 25-31) wherein

- The software system includes at least a filter which evaluates of a user for an access controlled object based on data which are not available until the time of access.(page 18, lines 24-30; figure 1, ref. Num "220") (A "filter" is interpreted by the office to be the "Permission code module 220" which is provided for evaluating the access rights of the user or the application for accessing the controlled objects or receiver functionalities or resources or user data under the control of the "Access Controller" as shown on figure 2, ref. Num "240" based on the data that are not available until the time of the access or "condition code module 225" as shown on figure 2, ref. Num "225" and as explained on page 19, lines 6-18)
- **The filter further evaluates additional data occurring while the user has access to the access control object**,[Page 20, lines 28- page 21; page 31, lines 19-28](Even If the caller has the required permission, a further check is made to determine whether a "condition" of the receiver 160 is satisfied. This is determined at the access controller 240 by analyzing the current environment of the receiver 160.] **monitors a change in the access rights**,[Page 21, lines 11-20; see also page 21, lines 21-page 22, line 14, page 31, lines 19-28] (data indicating the current environment of the receiver, such as time of the day or date, parental lockout status, pay-per-view status, current viewer, current authorization state that is relevant and changes over time.) and **triggering withdrawal of the access rights to the access controlled object.**[Page 22, lines 22-33] (If the access controller determines the condition/additional data which dynamically changes with time as explained on page 21, lines 19-20 while the user has access to the access objects as explained on page 20, lines 28-page 21, line 2 and monitors a change in the access rights as explained above and triggering withdrawal of the access right to the access controlled objects as explained on page 22, lines 22-23 or figure 3, ref. Num "370"]

4. **As per claim 3, Peterka** discloses a network as applied to claim 1 above. Furthermore, Paterka discloses a network, wherin in the software system, further comprises a resource manager which withdraws the access rights. (page 22, lines 22-31;figure 3, ref. Num "390")(the resource manger is interpreted by the office to be the "Access controller". After an application is used or after an application gets the first permission to the controlled object, the "Access Controller" continues to check the current condition dynamically for withdrawing the access rights as shown on figure 3, ref. Num "370" and explained on page 19, lines 6-18 and page 21, lines 11-31, page 22, lines 22-31)

5. **As per claim 4, Peterka** discloses a network as applied to claim 3 above. Furthermore, Paterka discloses a network, wherein the software system includes an access right manager which, together with the filter, is instructed by the resource manager to check the access rights.(figure 2, ref. Num "240", ref. Num "250" and ref. Num "220"; page 18, lines 24-30; page 19, lines 6-18; page 19, lines 24-31)

(The access right manager which is interpreted by the office to be the "Security Policy" which manages the access rights of the application as shown on figure 2, ref. Num "250" and the filter or the "Permission code Module 220" as shown on figure 2 are both controlled and instructed by the resource manager or "Access Controller" which is shown on figure 2, ref. Num 240" and explained on page 18, lines 24-30; page 19, lines 6-18; page 19, lines 24-31)

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. **Claim 5 and 6** is rejected under 35 U.S.C. 103(a) as being unpatentable over, **Peterka,** (hereinafter referred as **Peterka**)(International Publication Number: WO 99/66714) in view of "**Brown et al**. (hereinafter referred to as **Brown**) (U.S. Patent No. 5,941,947)

8. **As per claim 5**, **Peterka** discloses

- A network comprising a plurality of terminals and a software system distributed among the terminals, (page 13, lines 6-8; page 14, lines 20-24; figure 1, ref. Num "100", ref. Num "120"; ref. Num "160")(A network or the digital television broadcast network has the software system or the software application distributed or broadcasted to each terminals or receivers as explained on page 14, lines 20-24; the terminal is interpreted as "television receiver" and this interpretation is given in light of the submitted application as it is defined on page 3, lines 1-3) and

- A plurality of access control objects.[page 20, lines 15-18; page 4, lines 5-6) (controlled objects or functionalities and lists the name of the associated permission).

- The access right manage and the filter which evaluates access rights of the user to access the control objects, (A "filter" is interpreted by the office to be the "Permission code module 220" which is provided for evaluating the access rights of the user or the application for accessing the controlled objects or receiver functionalities or resources or user data under the control of the "Access Controller" as shown on figure 2, ref. Num "240" based on the data that are not available until the time of the access or "condition code module 225" as shown on figure 2, ref. Num "225" and as explained on page 19,

lines 6-18 and the access right manage is interpreted by the office as the "Security Policy" shown on figure 2, ref. Num "250") wherein

The access right manager which is interpreted by the office to be the "Security Policy" has a data structure for listing and accessing the permission of the associated controlled objects or functionalities and lists the name of the associated permission.(page 20, lines 15-18; page 4, lines 5-6). Furthermore Peterka discloses that "resource manager " which is interpreted by the office to be the "Access Controller" checks the access right manager or the "Security Policy" to check the appropriate permission.(page 19, lines 24-29)

Peterka does not explicitly disclose

A network as claimed in claim 4, characterized in that the access right manager (8) has a data structure in the form of a tree (15) for arranging access controlled objects (14) and in that the tree (14) includes a plurality of nodes (35 to 44) which each contain a list of permitted users or user groups respectively, of an access controlled object and for each user or user group respectively, include a list of methods of use.

However, in the same field of endeavor, **Brown** discloses that on-lines services or directory services maintains a directory structure of the content objects that are accessible to the user with the content objects forming nodes of the tree-like directory structure or data structure. This data structure provides a hierarchical navigable view of content. (column 2, lines 38-46)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to add the tree node data structure as per teachings of **Brown** in to the method taught by **Peterka,** in order to provide a data structure which has a

faster searching mechanism to access controlled objects or the requested functionalities and to accommodate and arrange a list of permitted users and methods in each node and accordingly provide a respond for the required permission efficiently.

9. **As per claim 6,** the combination of **Peterka and Brown** discloses a network as applied to claim 5 above. Furthermore **Peterka** discloses the network wherein **The filter further evaluates additional data occurring while the user has access to the access control object,**[Page 20, lines 28- page 21; page 31, lines 19-28](Even If the caller has the required permission, a further check is made to determine whether a "condition" of the receiver 160 is satisfied. This is determined at the access controller 240 by analyzing the current environment of the receiver 160.] **monitors a change in the access rights,**[Page 21, lines 11-20; see also page 21, lines 21-page 22, line 14, page 31, lines 19-28] (data indicating the current environment of the receiver, such as time of the day or date, parental lockout status, pay-per-view status, current viewer, current authorization state that is relevant and changes over time.) and **triggering withdrawal of the access rights to the access controlled object.**[Page 22, lines 22-33] (If the access controller determines the condition/additional data which dynamically changes with time as explained on page 21, lines 19-20 while the user has access to the access objects as explained on page 20, lines 28-page 21, line 2 and monitors a change in the access rights as explained above and triggering withdrawal of the access right to the access controlled objects as explained on page 22, lines 22-23 or figure 3, ref. Num "370"]

(10) Response to Argument

Applicant argued that the following limitation in the claim 1 is not disclosed by the reference on the record namely "Peterka, "**the filter further evaluates additional data**

occurring while the user has access to the access control object, monitors a change in the access rights, and **triggers withdrawal of the access rights to the access controlled object**."

Examiner disagrees with this argument.

Examiner would point out that Peterka **on page 30 lines 22-24**, discloses the fact that the invention uses **a dynamic approach to providing access control** which meets the limitation of evaluating additional data occuring while the user has access to the access control objects and also meets the rest of the limitation in claim 1. Furthermore Peterak further discloses the following facts.

"The filter further evaluates additional data occurring while the user has access to the access control object,[Page 20, lines 28- page 21; page 31, lines 19-28](Even If the caller has the required permission, a further check is made to determine whether a "condition" of the receiver 160 is satisfied. This is determined at the access controller 240 by analyzing the current environment of the receiver 160. **As explained on page 28, lines 17-31,** the user can define **the time frame for the childeren and access a certain program. This implies that while the childern has already access to the control object/program the system will monior the time and the current viewer whether or not the current viewer is a child or an adult**. This means the system inherently checks the identity of the viewer. The indentity of the user is checked by prompting the user to enter their approprate personal identification number **as explained on page 26, lines 26-31**.

Peterka further discloses how **the access controller determines who the current user is and checks his permissions as well as the application permissions monitors a change in the access rights**,[Page 21, lines 11-20; see also page 21, lines 21-page 22, line 14, page 31, lines 19-28 and page 30, line 22-24] (**data indicating the current environment of the receiver, such as time of the day or date, parental lockout status, pay-per-view status, current**

viewer, current authorization state that is relevant and changes over time.) and triggering withdrawal of the access rights to the access controlled object.[Page 22, lines 22-33; figure 3, ref. Num "370"] (**If the access controller determines the condition/additional data which dynamically changes with time as explained on page page 30 lines 22-23 and page 21, lines 19-20 while the user has access to the access objects as explained on page 20, lines 28-page 21, line 2 and monitors a change in the access rights as explained above and triggering withdrawal of the access right to the access controlled objects as explained on page 22, lines 22-31 or figure 3, ref. Num "370"] .**

The examiner points out the following facts. Peterka on page 31, lines 19-28 recites that, "when the user tunes to another chanel, sometimes the application stays on, and sometimes it is terminated, depending on the definiton of the policy" and this meets the limitaiton of monitoring a change in the access rights.

Therefore all elements of the limitations of claim 1 is disclosed by the references on the record.

The second argument by the applicant regarding claims 3 and 4

Applicants argument is based on the same reason provided to claim 1, since they are dependent on claim 1.

Examiners disagrees with the above remark by the same argument/reason/rational indicated for claim 1.

The other argument by the applicant is related to the independent claim 5.

Applicants argued that the references on the records namely Peterka, Brown and their combination does not include the following features and argued as follows:

"The cited text in Brown merely discloses that a directory service maintains a directory of content objects as nodes in a tree-like structure. However, the cited text makes no mention of each node containing a list of permitted users or user groups, respectively, of the access controlled object and for each user or user group

respectively, including a list of methods of use. Instead, it appears that Brown uses an access control matrix and access rights database (152) which is organized based on users, not by objects, and which is organized on a user-by-user (or user-group-by-user-group) basis to list for each user (or user group) the content nodes and access operations available to the user."

Examiner disagrees with this argument.

Examiner would point out that first of all the primary reference Peterka, on page 36, lines 13-15, points out the fact that the set of all **classes forms a tree,** where an Object is at the top. Furthermore Peterka discloses the access right manager which is interpreted by the office to be the "Security Policy" has a data structure **for listing and accessing the permission of the associated controlled objects or functionalities and lists the name of the associated permission**.(page 20, lines 15-18; page 4, lines 5-6). **Furthermore Peterka discloses that** "resource manager", which is interpreted by the office to be the "Access Controller", checks the access right manager or the "Security Policy" to check the appropriate permission.(page 19, lines 24-29) **and Brown discloses** that on-lines services or directory services maintains a directory structure of the content objects that are accessible to the user with the content objects forming nodes of the tree-like directory structure or data structure. This data structure provides a hierarchical navigable view of content. (column 2, lines 38-46) and **Brown on figure 3A and 3B** and **column 16 lines 55-59** discloses the following, "Each entry in the access control matrix 300 is in the form of a 16-bit access rights value (represented by the symbol "XXXX" in the figures), and specifies the access rights of a given user at a given node **(or equivalently, specifies the rights of a given user with respect to a given content object)".** The motivation of combing references as recited above is the following,

> It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to add the tree node data structure as per teachings of **Brown** in to the method taught by **Peterka,** in order to provide a data structure which has a faster searching mechanism to access controlled objects or the requested functionalities

and to accommodate and arrange a list of permitted users and methods in each node and accordingly provide a respond for the required permission efficiently. [See Brown on column 2, lines 47-66]

Applicant next argued the dependent claim 6 and the examiner response to the independent claim 5 also applicable to this particular claim. The last argument by the applicant in relation to the independent claim 7. The examiner response provided to claim 1 is also applicable to this claim since the examiner consider claim 7 to have similar limitation to claim 1.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

S.L.
Samson Lemma.

Conferees:

Gilberto Barron

Matthew Smithers

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100